REMARKS

I. Status and Disposition of the Claims

In the instant application, claims 1-15, 21-29, 32-34 and 40-43, of which claims 1, 21, 40 and 42 are independent, are pending and under consideration on the merits.

In the Office Action[1] mailed May 20, 2008, the Examiner took the following actions:

1) The Declarations filed by Applicant on February 6 2008, under 37 CFR 1.131 were determined to be sufficient to overcome U.S. Patent No. 7,017,186 ("Day"). Applicant notes this determination with gratitude.

2) Claims 1-7, 12-15, 21-28, 34 and 40-43 were rejected under 35 U.S.C. § 103(a) as being unpatentable over US Patent Application Pub. No. 2002/0083344 by Vairavan (hereinafter "*Vairavan*") in view of US Patent No. 5,796,942 to Esbensen (hereinafter "*Esbensen*").

3) Claims 8-11, 29, 32 and 33 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Vairavan* in view of *Esbensen* and further in view of US Patent No. 7,159,237 to Schneier et al. (hereinafter "*Schneier*").

II. Amendments to the Claims

In this response to the Office Action, Applicant amends claims 1, 4, 21, 23, and 40-43, and adds new claims 44-47.

---

[1] The Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicant declines to automatically subscribe to any statement or characterization in the Office Action.

Support for the amendments of claims 1, 21, 40 and 42 and new claims 44-47 may be found in the Specification at, for example, paragraph [0031], according to which

> [k]nowledge of the traffic profile, i.e. network statistics relating to protocols, hosts, and conversations, server & client response times, network Quality-of-Service conditions, historical traffic profile, and even actual packet traces, provide additional data points for security analysts in their endeavor to detect intrusion attacks. For example, if the IDS monitors a network parameter, it can determine when that parameter is outside of a normal, or expected range.... . A probe typically can be configured to record the number, duration, and amount of network traffic, and can categorize the traffic by protocols, hosts, and conversations, as well as other information specified in the various MIBs. This information can be made available to the IDS, and can be the basis for predetermined or user-specified alerts or action by the IDS.

Support for the amendments of claims 4 and 23 may be found in the Specification at, for example, paragraph [0039], which provides that "[i]f trunked traffic is received, the traffic is aggregated, that is, combined such that it appears to emanate from a single logical source (STEP 100)."

Applicant thus respectfully requests reconsideration.

III. Response to Rejections

A. The Rejection of Claims under 35 U.S.C. § 103(a) Should be Withdrawn.

In the Office Action, claims 1-7, 12-15, 21-28, 34 and 40-43 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Vairavan* in view of *Esbensen*. Applicant respectfully traverses the rejection of these claims in view of the amendments and following remarks.

"The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. . . . [R]ejections on obviousness cannot be sustained with mere conclusory statements." M.P.E.P.

§ 2142, 8th Ed., Rev. 6 (Sept. 2007) (internal citation and inner quotation omitted). "The mere fact that references can be combined or modified does not render the resultant combination obvious unless the results would have been predictable to one of ordinary skill in the art." M.P.E.P. § 2143.01(III) (emphasis in original). "In determining the differences between the prior art and the claims, the question under 35 U.S.C. 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious." M.P.E.P. § 2141.02(I) (emphases in original).

"[T]he framework for objective analysis for determining obviousness under 35 U.S.C. 103 is stated in *Graham v. John Deere Co.*, 383 U.S. 1, 148 U.S.P.Q 459 (1966). . . . The factual inquiries . . . [include determining the scope and content of the prior art and] . . . [a]scertaining the differences between the claimed invention and the prior art." M.P.E.P. § 2141(II). "Office personnel must explain why the difference(s) between the prior art and the claimed invention would have been obvious to one of ordinary skill in the art." M.P.E.P. § 2141(III).

For the above-cited claims, Applicant respectfully submits that a *prima facie* case of obviousness has not been established because the Office Action has not properly ascertained the differences between the claimed invention and the prior art. Accordingly, the Office Action has failed to clearly articulate a reason why the prior art would have rendered the claimed invention obvious to one of ordinary skill in the art.

With respect to claim 1, a *prima facie* case of obviousness has not been established because the claimed invention is not obvious as a whole. In particular, *Vairavan* and *Esbensen*, alone or in combination, fail to teach or suggest each and every element of claim 1. In addition, no additional evidence has been raised

establishing a tenable rationale that one of ordinary skill would have been motivated to modify the references so as to arrive at the claimed invention. For example, *Vairavan* fails to teach or suggest "transmitting, by the probe, over a second network line, data-converted packets and the updated historical network performance information, to an intrusion detection system, wherein at least one of the data-converted packets and the updated historical network performance information is used by the intrusion detection system to detect an intrusion on the first network link," and wherein the updated historical network performance information incorporates "current network performance data" collected by a probe, as recited in amended claim 1.

In rejecting claim 1, the Office Action cited *Vairavan* at paragraph [0090] as disclosing "monitoring, by the probe, the received packets to evaluate network performance." See Office Action at 3. In particular, at paragraph [0090], *Vairavan* recites a network intrusion detection mechanism that is configured to "[monitor] packets transmitted to or from specific devices on the enterprise" and perform "anomaly detections" by "compar[ing] usage characteristics of received packets" against a "pre-established baseline usage pattern." Applicant respectfully points out that paragraph [0090] of *Vairavan*, however, does not disclose detecting intrusions on a network link using "historical network performance information" which is updated with "current network performance data", as recited in amended claim 1. In contrast to "pre-established baseline usage pattern" disclosed by *Vairavan*, the network performance information, as disclosed by Applicant, is updated with "current network performance data" for intrusion detection purposes. *See* Applicant's specification at paragraph [0031]. The remaining sections of *Vairavan* also fail to disclose the recited elements of Applicant's amended claim 1.

Esbesen also does not make up for the deficiencies of *Vairavan*. *Esbensen* fails to teach or suggest systems and methods according to which "at least one of the data-converted packets and the updated historical network performance information is used by the intrusion detection system to detect an intrusion on the network link", as recited in Applicant's claim 1.

Moreover, one of ordinary skill in the art would not find it obvious to modify *Vairavan* in view of the teachings of *Esbesen* to achieve the required combinations recited by claim 1, when neither *Esbesen* nor *Vairavan* contain or suggest required elements recited in claim 1.

Here, Applicant respectfully submits that the Office Action has not explained *why* or *how* one of ordinary skill would modify the system of *Vairavan,* which provides an integrated network device (see *Vairavan* title), using the teachings of *Esbensen*, which provides a network surveillance system in which remote surveillance agents (RSA) capture network data traffic at several network locations (see *Espensen* col. 7, lines 19-23 and Fig. 4), so as to arrive at the claimed invention in which a probe is configured to transmit updated historical network performance information to an intrusion detection system, where the intrusion detection system uses the information to detect an intrusion on a network link. In particular, the Office Action has not explained at least: (a) *why* one of ordinary skill would modify the steps of *Vairavan* so as configure an intrusion detection system to perform intrusion detection based on updated historical network performance information and, especially, (b) *how* one of ordinary skill would know to select and arrange the steps of *Vairavan* and *Esbensen* so as to arrive at a system with the claimed feature of "transmitting, by the probe, over a second network link, data-converted packets and the updated historical network performance information, to an

intrusion detection system, wherein at least one of the data-converted packets and the updated historical network performance information is used by the intrusion detection system to detect an intrusion on the first network link," as recited in claim 1.

The burden is on the Patent Office to provide some tenable rationale as to *why* one of ordinary skill in the art would modify *Vairavan* using the teachings of *Esbensen,* so as to arrive at the presently claimed invention. In the present case, however, no such tenable rationale has been provided.

The Office Action provides a statement regarding incorporating features into a device:

> Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the method of Vairavan to transmit, by the probe, over a second network link, the packets to an intrusion detection system in communication with the second network link. One would be motivated to do so to accrue the benefits of a dedicated intrusion detection system as taught by Esbensen.

See Office Action at 4. However, these assertions do not demonstrate *why* or *how* one would modify *Vairavan*'s system with *Esbensen*'s features so as to arrive at the claimed invention. At best, the Office Action's position could be considered an assertion that the proposed modifications could be performed. However, "[t]he mere fact that a reference can be combined or modified does not render the resultant combination [or modification] obvious unless the results would have been predictable to one of ordinary skill in the art." M.P.E.P. § 2143.01 (emphasis in original). Combining *Esbensen* and *Vairavan* would not result in a predictable variation of Applicant's invention because *Esbensen* and *Vairavan* lack the elements recited in claim 1, namely "transmitting, by the probe, over a second network link, data-converted packets and the updated historical network performance information, to an intrusion detection system, wherein at least one of the data-converted packets and the updated historical network performance information is

used by the intrusion detection system to detect an intrusion on the first network link."

Further, even assuming *arguendo* that the Office Action's assertion is correct, having "a dedicated intrusion detection system" is not sufficient motivation for adding the specific elements of claim 1 to *Vairavan*. Further, nowhere in *Esbensen* or in *Vairavan* is there a suggestion of using a probe to transmit updated historical network performance information to an intrusion detection system for intrusion detection purposes. Therefore, both *Vairavan* and *Esbensen* miss the objective of the Applicant's system as recited in claim 1.

For at least this reason, a *prima facie* case of obviousness with respect to claim 1 has not been proven. Therefore, the rejection of these claims under 35 USC 103 as being obvious from *Esbensen* in view of *Vairavan* is thus improper and should be withdrawn.

Amended independent claims 21, 40, and 42, though of different scope from amended claim 1, recite similar elements and were rejected under the same rationale. See Office Action at 6. Therefore, for at least the reasons stated above with respect to claim 1, the *prima facie* case of obviousness for amended claims 21, 40 and 42 should be withdrawn.

In addition, claims 2-15, 22-29, 32-34, 41 and 43 are allowable at least because they depend directly or indirectly from claims 1, 21, 40 and 42.

B. Rejection of Claims 4 and 23 under 35 U.S.C. § 103(a) Should be Withdrawn.

A *prima facie* case of obviousness has also not been established with respect to amended claim 4 for at least the additional reason that *Vairavan* and *Esbensen*, alone or in combination, do not recite the claimed method of "aggregating the data packets received over the first network link and the data packets received over the third network link, wherein the aggregated data packet appears to emanate from a single logical source." In rejecting claim 4, the Office Action incorporated the rejections of claims 1-3, and further asserted, in reference to FIG. 1 of *Vairavan*, that "*Vairavan* further discloses the step of aggregating the data packets received over the first network and the data packets received over the third network." *See Office Action* at 4. At best, *Vairavan*'s network device 110 can collect data packets from "a plurality of network ports 115" connected to the device. See *Vairavan* at paragraph [0048]. However, Applicant respectfully points out that *Vairavan* does not disclose aggregating data packets in such a manner that "the aggregated data packets appear to emanate from a single logical source," as recited by Applicant's amended claim 4.

Esbensen also does not disclose aggregating data packets received over a plurality of network links, "wherein the aggregated data packet appears to emanate from a single logical source," as recited in Applicant's claim 4. In reference to FIGS. 4 and 5 of *Esbensen*, *Esbensen* discloses "RSAs [remote surveillance agents] 100a-c collect multiple packets on their attached WAN/LAN and compress multiple packets into a single internet packet which may be transmitted back through the WAN/LAN, over the internet, to RSS [remote surveillance server] 110." *Esbensen*, col. 7, lines 35-39. However, each one of "RSAs 100a-c" in *Esbensen* is connected to a single WAN/LAN

and is utilized to compress packets from that single network link. See *Esbensen*, FIG. 4. In contrast, Applicant's claim 4 discloses aggregating data packets received from a plurality of network links, where the "aggregated data packet appears to emanate from a single source." The remaining sections of *Esbensen* also fail to disclose such subject matter. For at least these reasons, the *prima facie* case of obviousness with respect to claim 4 should be withdrawn.

Amended claim 23, though of different scope from claim 4, recite similar elements and was rejected under the same rationale. See Office Action at 6. Therefore, for at least the reasons stated above with respect to amended claim 4, the *prima facie* case of obviousness of claim 23 should be withdrawn.

C. The Rejection of Claims 8-11, 29, 32 and 33 under 35 U.S.C. § 103(a) Should be Withdrawn.

Claims 8-11, 29, 32 and 33 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Vairavan* in view of *Esbensen* and further in view of *Schneier*. In rejecting these claims, the Office Action stated that

> [I]t would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of *Vairavan* to further include the steps of maintaining, by the probe, an audit trail buffer for forensic analysis; wherein the audit trail buffer comprises a memory for recording monitored packets; wherein the memory records packets from at least on of the first network link and the third network link; upon receiving, by the probe, an even notification, communicating, by the probe, the current contents of the audit trail buffer. One would be motivated to do so to reduce the amount of information to be processed by the central intrusion detection system as known to one of ordinary skill in the art.

See Office Action at 7. Applicant submits that a prima facie case of obviousness has not been established for at least the additional reason that modifying *Vairavan* to

incorporate the features of *Esbensen* and *Schneier* would not result in the invention recited in claim 8-11, 29, 32 and 33 as a whole.

Claims 8-11, 29, 32 and 33 depend from claim 1 and 21 and thus include all the elements and limitations thereof. As set forth above with respect to claim 1, the feature of "transmitting, by the probe over a second network link, data-converted packets and the updated historical network performance information, to an intrusion detection system," is not disclosed in *Vairavan* or *Esbensen*. *Schneier* also does not teach, disclose or suggest this feature. The probe disclosed in *Schneier* is configured to collect data from a network component, such as a "firewalls and intrusion detection system" and transmit any "noteworthy information" to off-site security analysts for intrusion detection. See *Schneier* at col. 4, lines 48-63, and col. 5, lines 38-43, particularly the arrow in FIG. 1 from Firewall and Intrusion Detection Systems 1010 to probe 2000. However, nowhere in *Schneier* is there any suggestion of "transmitting, by the probe, ... data-converted packets and the updated historical network performance information, to an intrusion detection system," as recited in claim 1 (Emphasis added). Therefore, whether or not *Schneier* discloses the features recited in claims 8-11, incorporating these features into *Vairavan* in view of *Esbensen* would not result in a system with the features recited in claims 8-11 as a whole.

Further, even assuming *arguendo* that the Office Action's assertion is correct and assuming *arguendo* that *Vairavan* and *Esbensen* are combinable, "reduc[ing] the amount of information to be processed by the central intrusion detection system" is too general a motivation to suggest adding the specific elements claimed in claims 8-11 to a hypothetical networking device of *Vairavan* combined with *Esbensen*. Further, nowhere in *Schneier* is there a suggestion of transmitting historical network performance

information to an intrusion detection system, "wherein at least one of the data-converted packets and the updated historical network performance information is used by the intrusion detection system to detect an intrusion on the first network link," as recited in claim 1.

For at least this reason, a *prima facie* case of obviousness with respect to claims 8-11 have not been established. The rejection of claims 8-11 under 35 U.S.C. §103(a) is thus improper and should be withdrawn.

For at least the reasons noted above, claims 29, 32 and 33, which recite similar elements rejected under the same rationale, are allowable under 35 U.S.C. §103(a). See Office Action at 8.

IV. New Claims 44-47 are in Condition for Allowance.

As set forth above, claims 1 and 21 are allowable. Therefore, new claims 44-47 are also allowable at least because they depend directly or indirectly from claims 1 and 21.

V. Conclusion

In view of the foregoing response and remarks, Applicant respectfully requests the reconsideration and reexamination of this application and the timely allowance of the pending claims. Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

Dated: August 20, 2008

By: 

Maura K. Moran
Reg. No. 31,859